

Andrzej Jankowiak*

THE SAFETY OF ELECTRONIC COMMUNICATION IN INTERNET BANKING

1. The Significance of Electronic Communication in Internet Banking

1.1. Electronic Communication in an Information Society

The information society is a society in which information is an essential element. The Report of the I Polish IT Congress from 1994 defines such a society as computerised and using telecommunication services to transmit and to remotely process information¹. The material and organisational basis is an IT net, which makes electronic communication possible. The information society is commonly mistaken with a strategy related with dissemination of Internet availability. The main difference is that information society is based on information, while Internet is a tool used to transmit that information and is a source of getting information.

The changes in employment, which took place in the economy, were directed to transfer employees from industrial sector to services. The issues indissolubly connected with information society gained on importance. Those issues are remote trainings, telejob, IT services, computerisation of public administration. Together with development of the Internet, it was hoped to increase profits generated by contemporary enterprises. However, the dissemination of IT, including the Internet, did not lead to constant economic growth, as it was expected. The economy and market law turned out to be invariable. The development of the Internet strengthened only tendency of orientation to the market and to the client's needs².

* The author is preparing a PhD thesis in the Chair of Banking at the University of Economics in Poznań under the supervision of Professor Alfred Janc.

¹ Raport I Kongresu Informatyki Polskiej, Poznań 1994, http://www.kongres.org.pl/online/1-szy_Kongres/index.html (28.05.2009).

² A. Dzikowski, E. Radosiński, *Internet a orientacja strategiczna przedsiębiorstwa*, w: *Koncepcje zarządzania przedsiębiorstwem*, red. L. Pacholski, S. Trzcieleński, Instytut Inżynierii Zarządzania Politechnika Poznańska, Poznań 2003, s. 26.

The usefulness of the electronic banking is noticeable for all its users. The entrepreneurs got a new channel for inserting their advertisements and presenting their offer. This is a channel which is not limited by any territorial borders. When the Internet appeared, the bankers created electronic banking, which opened new possibilities for contacts with the client. Thanks to the electronic communication, the realisation of a bank transaction became quicker. At the same time, the costs of transaction decreased and the banks could offer new products and financial services.

The state administration obtained the possibility to communicate with the client in an electronic way, to electronically inform people about tenders and planned ventures and about changes in law acts.

With higher level of informatisation (IT systems), private people started to get benefits from the possibilities offered by the global Internet network. It was possible thanks to, among others, reduction of computer equipment prices and extension of infrastructure of IT nets. We can observe incredible popularity of e-mails, communicators, VoIP telephone net, shopping in Internet shops and transfers via electronic banking.

The benefits of electronic communication were gathered by W. Cellary. He divided those benefits into 4 main characteristics of realisation of business processes through computer net³:

1. Time – the realisation of processes with the usage of computers connected by Internet takes much less time than doing the same thing with traditional methods. The time needed to get widely understood information got significantly shorter. As a result, the effectiveness of activities much improved.
2. Costs – lower cost of realising a transaction in an electronic way comparing with traditional way. Reduction of engagement of human work.
3. Geography – the electronic communication is independent on a distance. There is no difference in sending an e-mail to the room next door and to another continent.
4. Automatic reaction – thanks to identification of a person with the usage of profile data base, the business service process can be automatically personalised in order to fit appropriate offer.

As it was mentioned before, the development of IT technologies in the scope of communication brought new possibilities to banking and

³ *Polska w drodze do globalnego społeczeństwa*, red. W. Cellary, Program Narodów Zjednoczonych ds. Rozwoju, Warszawa 2002, s. 30.

financial sector. It resulted in creation of the electronic banking, which is defined in a literature as a form of delivering and providing bank services with the usage of remote access channels. Thanks to the electronic channels of access, the client can stay at home and make bank transaction using a telephone or a computer.

1.2. The Electronic Banking as Contemporary Trend in Banking

The development of IT technology and dissemination of access to Internet brought changes to banking. That process has been noticeable since the end of 1990s. The society started to use computers more and more commonly. Previously, the computers supported human's work and facilitated it. Then, also electronic communication became increasingly popular, because it made the communication and trade transactions easier. It was obvious that such a communication was independent on distance between both parts of communication. Suddenly, huge, global market, bound with IT net, became open. The bankers also saw those tendencies and introduced electronic banking. The competitiveness on the banking market forced the banks, which wanted to remain in economic reality, to make investments quickly and adjust themselves to that trend.

The electronic banking was defined in a literature as a form of providing bank services with usage of remote access channels⁴. The application of IT technologies caused that a client did not have to visit traditional bank branch in order to make a financial transaction. Having a computer with Internet access, they could make it from their home or any other place. A. Janc and G. Kotliński indicated various systems composing electronic banking, it is among others: telephone systems, systems enabling to do a transaction, systems for non-cash payments, cash machine systems and IT systems⁵. Taking into consideration the mentioned systems, one can classify them into two categories: internal and external ones. Internal systems comprise the whole infrastructure functioning in a bank, while external systems concern distribution of products and bank services to the client. Those external systems, composing electronic banking, are the subject of an analysis in the hereby article.

⁴ A. Nosowski, *Geneza bankowości elektronicznej*, w: *Bankowość elektroniczna*, red. A. Gospodarowicz, Polskie Wydawnictwo Ekonomiczne, Warszawa 2005, s. 26.

⁵ A. Janc, G. Kotliński, *Wykorzystanie bankowości elektronicznej w rozwoju usług*, „Bank” 1999, nr 9, s. 33.

The origins of electronic banking reach sixties years, when in the United States of America people started to use first cash machines. The next step was giving facility of telephone service of bank accounts. Only in eighties, people started to use computers to provide bank services. Those computer related services were limited, at the beginning. The first bank which used Internet in communication with its clients and in realising transactions was La Jolla Bank FSB from California. The Bank offered such solutions for the first time in the year 1994. The next Internet bank, Security First Network Bank, had started to provide such services since October 1995. In turn in Europe, Scandinavian banks were the leaders of electronic banking – those were Finish and Swedish banks⁶. In Poland, Internet banking began to develop in the 1990s, mainly though cash machines belonging to the bank PKO BP. Whereas, the banks from Pekao SA Group were the first banks providing services via Internet. In 1998, the Group created the Electronic Department in Łódź city⁷.

The classification of tools of electronic banking used in communication with a client includes telephone banking, cash machines, home banking and virtual banking. Telephone banking is one of the oldest forms of electronic banking. It allows the client to make transactions on their bank account with usage of traditional telephone or mobile phone. This form of electronic banking became popular due to broad availability of telephone devices as they were used in every day life and due to simplicity of telephone's usage. The literature indicates on various forms of providing services in telephone banking. The first form concerns services provided automatically, where the system plays previously recorded voice statements and the client guides the system with telephone buttons. The whole system is controlled by a special computer software. The second form of providing services concerns access by an operator to whom one orally says their orders⁸. The other popular way of access to electronic banking is with mobile phones. In that case, the communication of a client with a bank is realised by, among others, SMS messages. The banks offered also access to electronic banking via WAP technology. This technology adjusted Internet web pages to mobile phones. The web

⁶ D. Dziuba, *Systemy informatyczne w obsłudze banków detalicznych*, Katedra Informatyki Gospodarczej i Analiz Ekonomicznych Wydziału Nauk Ekonomicznych Uniwersytetu Warszawskiego, Warszawa 2002, s. 182.

⁷ <http://media.pekao.com.pl/pr/28659/historia-banku-pekao-sa-w-pigulce> (02.05.2009).

⁸ B. Świecka, *Bankowość elektroniczna*, CeDeWu, Warszawa 2004, s. 19.

pages are in such case shown on the screen of a mobile phone in simplified version, providing nevertheless the same functionality as in case of computers connected to transactional system of a bank⁹.

The second channel of distribution of electronic banking services are cash machines. The machines enabled people to pay out the cash with special cards given to bank accounts. The cash machines offer also printing out confirmations of transactions done, information about balance on an account, and sometimes even enable to pay cash into the account. Thanks to the cash machines, the clients gained continuous access to their cash without necessity to look for a bank branch. The branches are then passed over which results in lower costs of their maintenance¹⁰.

The third component of electronic banking is home banking. Its popularity increased together with dissemination of PC computers. At the beginning, that kind of solution was mostly common in big and medium sized companies. The main feature of home banking is a special software, which is installed on the user's computer. In order to communicate with a bank through home banking one has to own a computer, access to Internet or telephone line and a printer¹¹. Apart from hardware, also software plays an important role. It is software, which guarantees high level of security and which led the whole system to success. Together with development of IT technologies, the software which on one hand was the reason of success, on the other hand became its big disadvantage as the years went by. It is because the client can use home banking system only on the computer with the software installed by a bank specialist. The home banking is most often installed on office computers. As a consequence, one cannot get access to the bank from any other place, like home for example. In times when mobility and flexibility plays an important role, home banking started to lose its popularity.

Another channel of distribution of electronic banking services is an Internet bank. All the transactions in such a bank are made with the usage of a computer connected to the Internet. The Internet banks generally do not have traditional branches. They operate only in the Internet. Their offer is diversified and depends only on internal policy of such a

⁹ M. Marcinkowska, *WAPorujące usługi bankowe*, „Bank” 2001, nr 1, s. 75.

¹⁰ G. Kotliński, A. Rzeźnik, *Kanały dystrybucji usług bankowości elektronicznej*, w: *Nowe technologie we współczesnym banku*, red. A. Janc, G. Kotliński, Akademia Ekonomiczna w Poznaniu, Poznań 2004, s. 315.

¹¹ P. Tomala, *Systemy home bankingowe*, „Bank” 2002, nr 7-8, s. 64.

bank. Recently, the banks enlarged their offer and now, apart from strictly financial services, one can find also offer of insurances, investment and retirement funds or broker services. Moreover, placing on a bank's web site additional information like currency exchange rates table and important economic news makes such a site also a news service¹².

In Poland, it was mBank which was the first fully virtual bank. The first clients opened their accounts in November 2000. In spite of preliminary distrust to modern form of banking, in March 2002 the number of clients using mBank's electronic banking reached half million¹³.

Apart from the banks typically virtual, there are also traditional banks, which create an electronic department or only support their activity with electronic channels of distribution¹⁴. Such actions are caused, on the one hand, by competitive banks on the market, and on the other hand, by willingness to use recognisable brand in order to increase share on the bank services market.

1.3. The Significance of Safety and Trust in Electronic Communication

The safety of electronic communication means both prevention from doing any action through electronic channels by an unauthorized person, and protection of transmitted information from its distortion in the process of transmission. The safety may also concern protection from getting to know the content of transmitted information by not involved persons, as well as marking sent documents with date and hour. Time marking concerns the moment of creating and signing the electronic document.

Dissemination of electronic communication led to sudden increase in number of transactions done in electronic way. Such transactions are done in electronic banks, Internet shops, Internet auctions or directly through e-mail correspondence. In each of those cases, the crucial factor of positive realisation of a transaction was safety of communication, which was a kind of guarantee. The issue directly connected with safety of the electronic transaction is trust to, so called, the other part - it

¹² J. Grzechnik, *Bankowość internetowa*, Internetowe Centrum Promocji, Gdańsk 2000, s. 40.

¹³ T. Koźliński, *Bankowość internetowa*, CeDeWu, Warszawa 2004, s. 48.

¹⁴ D. Garczyński, *Formy organizacyjne bankowości elektronicznej*, w: *Bankowość elektroniczna*, red. A. Gospodarowicz, Polskie Wydawnictwo Ekonomiczne, Warszawa 2005, s. 43.

may be contractor, computer system realising an order or an operator, who is an unknown person.

The Internet shops run activity virtually, it is through WWW web pages. On those pages there are products and commodities, as well as mechanism for ordering products. The Internet shops offer the possibility to pay for purchases in connection with transactional systems of the electronic banks. The safety includes in that case clients' personal data, which are transmitted, confirming the identity of other part of transaction and authorising the electronic payments in case when a number of bank card is given.

Analysing the motives of the clients, when they do electronic purchases, one can divide the clients into those who do transactions – they go only by a price of a product, and those who build relations – they look for friendly and certain companies which offer checked and reliable products. Such clients will co-operate with the company for a long time. The trust is precisely the basis of building such a loyalty¹⁵.

Electronic communication, used in various forms, is exposed to various types of risks, due to its virtual character. Those risks concern both security of transferred data, and users' trust to virtual organisations. In case of Internet shops, the security issue concerns personal data transferred. In the electronic banking the risk is bigger, because it concerns not only personal data, but also anxiety about money theft. Breaking security passwords, a hacker (an Internet thief), gets also access to accounts and credit cards numbers. The threats to electronic communication change, as well as the possibilities offered by electronic communication change.

Generally, the importance of trust increases significantly in case of immaterial goods and virtual institutions. The trust is then strictly connected with credibility, which those institutions gain from clients. People which communicate electronically through Internet, become much less emotionally bound with each other. There is no such relationship, which normally arises in personal contacts. The people do not also get used to each other or to a place. Moreover, there is a need to give one's personal data in order to finalise a transaction. As soon as a client notices lack of a factor guaranteeing expected stabilisation, he will reduce or even resign from further cooperation.

¹⁵ F. Newell, *Lojalność.com*, IFC Press, Kraków 2002, s. 56.

It was lack of trust and safety consciousness, which became a crucial factor of clients' resigning from doing electronic transactions. Not all Polish companies use appropriate electronic protections, which fact only confirms the clients' anxiety. Internet became an anonymous place, what makes the problem of trust in electronic communication bigger. The trust has to surpass the level of risk beard by the client. All the information about implementation of additional protection tools have always positive perception, even if they increase the safety of electronic communication only in small extent.

2. Threats to Information Transfer in Electronic Communication

2.1. The Classification of Threats to the Security of Communication with the Client in Electronic Banking

At the origins of electronic banking, the web sites of banks served only for their presentation, promoting bank's image and were the place of cheap advertisement. Moreover, the sites were used for informing the clients about changes in the offer and for presenting financial data such as, for example, currency exchange rates. Soon, such an attitude towards web sites changed and developed in the direction of active access to the banks' products. Thanks to that the clients gained full access to their bank accounts and possibility to carry out wide range of transactions¹⁶. The tendency of mobility on the market resulted in implementing more and more IT solutions, including wireless access to the Internet.

The strategy of implementing IT in bank operation on the one hand required bearing investment costs for modernisation of computer systems, on the other hand it generated income from activity on the electronic market. As a result of that strategy, one could observe significant increase of functionality of distribution channels of bank services. Nevertheless, at the same time, the safety of communication between a bank and a client became more threatened. The threats existing so far only in the IT sector became also threats to the bank systems. Hackers which earlier were interested only in breaking into the electronic post and illegal modifying software, got concentrated on activities bringing them financial benefits. They started to attack without any permission sites, where money in the electronic form was located.

¹⁶ A. Jurkowski, *Bankowość elektroniczna, Materiały i studia, Zeszyt nr 125*, Narodowy Bank Polski, Warszawa 2001, s. 55-63.

Specific activity of Internet banks made the need for guaranteeing high level of security of electronic financial transactions have double significance. On the one hand, it is necessary to eliminate the access of unauthorised persons to the money gathered by an electronic bank. On the other hand, it is important to build trust to an institution which very often has virtual character. It is because, the main value of an Internet bank is its brand and established renown. Those values may be negatively influenced by information given publicity, that there were attempts of an electronic break-in. That is why the banks, having in mind that the trust is crucial, often try to hide information about such attempts from media, and reimburse the losses to the clients affected by electronic robbery without even searching for a guilty person – the client, who unknowingly made their access password available or a hacker, who broke that password.

It is worth noticing that in case of electronic banking users, the level of security of data transmission in the electronic communication is influenced by the computer equipment and operational system, which electronic transactions are made on. The danger is caused by:

- computer viruses – pseudo programs created in order to cause harm on infected computer,
- Trojan horses – codes hidid in a program, which make the program perform different, negative functions from the original ones,
- hacker attacks – gaining unauthorised access to a computer thanks to errors in a software.

In spite of logic, serious danger for the electronic data is also generated by the human being. It results from inattention and naivety, and sometimes even malicious actions. The entrepreneurs use to save money on trainings about computers and data security. It may have result in the security of the whole IT system of the company.

The Basel Committee on Banking Supervision became an international institution acting for improving standards of banking supervision. The Committee was founded with participation of representatives of central banks from selected countries. The standards and recommendations created by the Committee do not have compulsory character. Supervisory

authorities from each country decide by themselves whether to implement them into domestic legislation or not¹⁷.

The Basel Committee noted appearance of brand new categories of dangers to the electronic banking in comparison with the traditional ones. Those risks were gathered in the document called "Risk Management for Electronic Banking and Electronic Money Activities". The main risk category indicated in this report is operational risk, which means possibility to generate losses due to lack of compactness or safety of the electronic banking systems. Within the operational risk the Committee distinguished three subgroups. The first concerns security risk and is connected with data transmission and access to the bank systems. The second subgroup concerns risk of system's design and development, which is connected with incompatibilities arising from changes in system of client-bank communication. The last subgroup refers to risk arising from inappropriate usage of bank products and services by the client¹⁸. Apart from the operational risk, the Basel Committee indicated also on reputation and legal risks. The first risk concerns influence of an error on public opinion. Bank's recognition and good brand can be negatively affected by computers' break down or overload, as well as hackers' attack. The bank's position and trust to it may be also shaken in the situations: when the client does not have full access to the system, when the bank does not answer on client's questions or when the bank does not publish important information. The second – legal risk – refers to confidentiality of clients' data, which may be sometimes revealed to unauthorised persons¹⁹.

Basing on the recommendations of the Basel Committee, the General Inspector of Banking Supervision issued Recommendation D, concerning management of risks related to the IT and telecommunication systems used by the banks. That document obliges the banks, among others, to set management control over risks and moreover, to create security policy and detailed regulations referring to those risks. Additionally, the banks should use securities for IT systems taking advantage of specialised software and technical possibilities of hardware. The recommenda-

¹⁷ M. Koterwas, *Bazylejski Komitet ds. Nadzoru Bankowego i jego wpływ na kształt nadzoru bankowego na świecie*, „Bank i Kredyt” 2003, nr 10/2003, s. 58.

¹⁸ Risk management for electronic banking and electronic money activities, Basle Committee on Banking Supervision, Basle, Marzec 1998, s. 5 i nast.

¹⁹ J. Górka, *Specyfika ryzyka bankowości elektronicznej, Materiały i studia*, Zeszyt nr 205, Narodowy Bank Polski, Warszawa 2006, s. 36.

tion requires using appropriate methods to make it impossible to neglect having made the transaction and to bring in responsibility for the transaction made with usage of electronic banking²⁰.

The Recommendation D describes four issues²¹: the role of bank's authorities in managing the safety of IT systems, mechanisms of security control, managing risks, IT audit and supervision. The requirements result from variety of IT systems used by banks, and even from diversity of risk existing in particular banks. That is why it was required to adjust the methods to the scale of threat.

2.2. The Methods of Protecting the Electronic Communication in Internet Banking

In order to reduce or wholly eliminate the dangers to the security of the electronic banking, the bankers and IT specialists continuously up-date and improve transactional systems. The literature concerning this subject gathers the most important security requirements, which should be fulfilled in communication with the client in the electronic banking²²:

- possibility to confirm the identity of a client, who makes a transaction,
- system of coding the data transmission and guarantee of confidentiality,
- securing the server of financial services provider from illegal access,
- securing the bank's server from deliberate attacks launched from outside (Internet) and from inside of the bank (local net).

The electronic banking is a specific kind of electronic communication, which is also the most exposed to risk in the scope of security. That is why, it is necessary to use all the possible legal and technical means in order to ensure the highest possible level of security and trust to financial institutions, especially when they operate virtually.

²⁰ K. Maćkowiak, *Bankowość elektroniczna – korzyści i zagrożenia*, „BOSTON IT Security Review” 2007, nr 4, s. 14.

²¹ Zob. Rekomendacja D dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki, Generalny Inspektor Nadzoru Bankowego, Warszawa 2002.

²² P. Nowakowski, M. Toporowski, R. Tylski, *Bezpieczeństwo transakcji finansowych przeprowadzanych za pośrednictwem kanałów elektronicznych*, w: *Nowe usługi finansowe w Polsce*, red. W. Przybylska-Kapuścińska, U. Ziarko-Siwiek), Akademia Ekonomiczna w Poznaniu, Poznań 2002, s. 76.

There are various technical methods of reducing risk in electronic communication. The banks use passwords, tokens, as well as more and more often an electronic signature in order to electronically verify the communication with the client.

Generally, one can distinguish verification by one factor and many factors. The first type refers to identification by only one factor, for example password, while the second type makes use of combination of two or more methods of verification.

The password became the basic element which guarantees safety of client's access to the bank's electronic system²³. It is the simplest protection mechanism and the cheapest at the same time. We distinguish many different forms of password's construction (series of signs composing the password) and many mechanisms of entering the password in the system. The password should be difficult to guess. It should be a combination of letters, numbers and special signs. Moreover, the password should be regularly changed and, most of all, disclosed to nobody. There are different manners of putting the password into banks' systems. One can enter the full password or, so called, camouflaged password - it means entering only some selected signs from the password. Usually, in the camouflaged method, the system each time asks about another set of signs from the password.

The password serves for identification of the user and allows them to get access to the system. Nowadays, the password itself does not guarantee appropriate level of safety. Due to the fact that the password may be spied or taken over by a virus, such as a Trojan horse, the possession of password should not make it possible to do any transaction. The only option, permissible thanks to the password, ought to be browsing the data.

One of the password types is a one-off password. It usually serves for confirming the actions done in the electronic banking system. One-off passwords serve for authorisation of banking operations and are delivered to the client in a form of printout. Their one-off character eliminates the risk of being spied by unauthorised persons during the transfer, because once the password is used, it expires. There is special kind of passwords – an SMS password, which is sent to the user's mobile phone at the moment of authorisation of a transaction. This password also expires, once it

²³ www.ingbank.pl/u235/navi/56117 (18.07.2009).

is used²⁴. The same feature is characteristic for an electronic device, called token, which generates a series of numbers. The password generated by token may be used only once for confirmation of one electronic transaction. Token uses cryptographic algorithm in its work²⁵. The presented tools may be voluntarily chosen by the client, who communicates with the bank.

The combination of the one-off password with the camouflaged password can be an efficient manner of increasing the level of safety. The first of those two passwords may be theoretically stolen, but the client additionally enters the second password, which is known only to themselves. Moreover the camouflaged password is entered in camouflaged version, which means that spying the whole password would take a hacker a lot of time.

The authorisation of transactions can be also done with the usage of a microprocessor card. Such a card is protected with a password from access. Moreover, the card enables records on it and unauthorised reading of the data. The card is connected with a particular bank account. It can also be a carrier of a password or an electronic signature. The usage of an electronic signature guarantees the highest level of safety of transaction's authorisation. It assures immutability of a disposition sent electronically to the bank's system.

Generally, the authorisation can be conducted by:

- an element known to the user, it is for example the password,
- what the user has in their disposal, it is the microprocessor card,
- characteristic features owned by each particular person, it is biometric.

In comparison with a password, the biometric features cannot be stolen or falsified. One cannot also lose them. It is expected that biometrics will revolutionise the methods of user's identification in the IT systems.

Moreover, in the electronic transactions, not only bank related, one uses the SSL protocol with 128-bits coding key in order to ensure secure communication in the Internet. The SSL protocol includes a set of

²⁴ www.mbank.pl/przewodnik/bezpieczenstwo/porwnanie_hasel_kodow.html (18.07.2009).

²⁵ www.lukasbank.pl/oferta_ekonto_bezpiecz_token.asp (18.07.2009).

orders and standards allowing safe exchange of information between an Internet browser and the bank's server²⁶.

The issue of security and trust to bank's electronic transactions found its place in Polish legal acts, among others in the Act about Electronic Payment Instruments from 12 September 2002. This act includes a whole chapter concerning the electronic banking, which name is "The Electronic Banking Services". The electronic banking was treated as an electronic payment instrument. It was defined in details in article 29 of the above Act, which says that the bank is obliged to assure the access to money funds gathered on an account using the wire and remote devices possessed by the account owner, as well as do the transactions and other activities ordered by the client²⁷. Assuring the access means guaranteeing safe control over the money funds gathered on the account.

Nevertheless, it is important to emphasise that even using all of the above mentioned security tools does not relieve the client of an Internet bank from being cautious. The client should very carefully protect their password to the bank account, check whether the computer is protected with appropriate and continuously up-dated software programme guaranteeing the security of communication in the Internet. Moreover, the client should verify whether electronic transactions were done in coded connection.

3. The Chance for the Electronic Signature in the Scope of Authentication of the Communication in Internet Banking

3.1. The Electronic Signature, its Features and Advantages

According to the Electronic Signature Act, that kind of signature means electronic data which, in combination with the other data to which they are added to or with which they are logically linked, serve for identification of a person setting the electronic signature²⁸. That definition was based on the text of the directive concerning the union frames in the

²⁶ M. Gadzińska, *Metody szyfrowania informacji wykorzystywane w zarządzaniu bezpieczeństwem informatycznym w banku*, w: *Nowe technologie we współczesnym banku*, red. A. Janc, G. Kotliński, Akademia Ekonomiczna w Poznaniu, Poznań 2004, s. 137.

²⁷ Rozdział 4 Ustawy z dnia 12 września 2002 roku o elektronicznych instrumentach płatniczych (DzU z 2002 r., nr 169 poz. 1385).

²⁸ Art. 3 ust. 1 Ustawy o podpisie elektronicznym z dnia 18 września 2001r., (Dz.U. Nr 130, poz. 1450).

scope of the electronic signatures²⁹. The directive was elaborated by the European Parliament and the Council of European Union as a determinant of the conditions, which the legislation of the UE members in that scope should be compliant with. Both the directive, and the Polish Electronic Signature Act characterise with technological neutrality of the signature. It means, among others, that they allow every method of electronic authorisation. Implementing joint legal rules standardising the electronic signature was necessary to harmonise the flow of commodities and services on the UE markets. Thanks to that document, the electronic signature became acceptable by legal systems of all member countries.

The aim of a Polish legislator was to equalise the electronic signature with the manual signature in the scope of legal effects. Articles 78 of Civil Code and article 5 point 2 of the Electronic Signature Act state about that. Only a secure electronic signature causes the same legal effects as a manual signature. Such an electronic signature meets following conditions³⁰:

- unequivocal identification of a person who sets the signature,
- unrepeatable character,
- it is created with the usage of devices and private key – only the person who sets the signature has access to that key,
- allows detection of attempts to change the data, which the signature is bound with.

It is important to remember that although the signature originates from the cryptography of asymmetric key, it does not aim to code the whole message. Only an abbreviation of the message is coded. That abbreviation, together with user's private key, creates the electronic signature of the signed document. The characteristic feature of the message's abbreviation is that each change of the message's text results in change of the abbreviation. Moreover, there is no possibility to reconstruct the message on the basis of the abbreviation.

The verification of the signature is done through decoding the signed abbreviation using the public key and then comparing the abbreviation with the one created out of the message. If they are identical, the

²⁹ Zob. Dyrektywa 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz.Urz. WE L 13 z 19.01.2000).

³⁰ Art. 3 ust. 2 Ustawy o podpisie elektronicznym, op. cit.

signature is recognised as valid³¹. The fact that everyone who owns the public key can decode the abbreviation means that the signature is not a method of keeping the message secret. However, the electronic signature is an excellent way to irrefutably confirm that the document comes from the person who signed it.

The electronic signature consists of:

- private key, which serves for signing and is possessed by its owner,
- public key, which is used to check the propriety of the signature made on the electronic abbreviation of the document. The public key is available publicly to all the persons interested in having it.

The last element necessary to verify the signature is a certificate of the public key, it is an electronic attestation which certifies that the key belongs to a particular person. If the certificate was issued by the entity registered by the Ministry of Economy, it means that the certificate is qualified. The certificate confirms the compatibility of the electronic key by indicating the connection between the private key with the public key. Only secure electronic signature, verified with the usage of qualified certificate, meets the requirements to be equal with manual signature.

Among the most important advantages of the electronic signature, we can indicate guaranteeing the safety of electronic transactions by assuring the invariability of the message's text. Moreover, the electronic signature allows us to easily confirm the identity of a contractor without necessity to examine the signature by graphologists, as it is done in the case of manual signatures. Another advantage is also the fact that the electronic signatures have common legislation and are bilaterally recognisable in Poland and in the world. The opportunity for that kind of signature is continuous increase of knowledge about the electronic transactions and of interest in issue of safety of the electronic communication. Weak point of the signature is the need for outlays and for adjusting the computer hardware to the requirement of a software used to set signatures. What is considered as a serious threat to the electronic signature is a common lack of trust in the society to virtual transactions on the contrary to still preferred paper transactions.

³¹ *Podpis elektroniczny. Komentarz do ustawy z 18 września 2001 roku*, red. J. Przetocki, Lexis Nexis, Warszawa 2002, s. 37.

3.2. The Electronic Signature as the Answer to the Needs of Internet Banking

There are many methods of authorisation of electronic transactions in Internet banks. Some of them were described above. All of those methods could be replaced by one secure electronic signature. The problem is that it would have to be accepted by all banks. The number of passwords, which a client has to remember, would limit to only one access password to the signature. The success of implementing the technology of the electronic signature into broad usage in banking depends mainly on big banks. Only if big financial institutions decided to implement the electronic signature, the tendency of transactions' security would change on the market. Other financial institutions would have to adjust to the standards on the market and to current tendency in security in order not to loose their worked out market positions.

It is important to remember that the aim of authorisation of electronic transactions has triple character. Firstly, the client will have a confirmation of placing the order. Secondly, the bank will have a confirmation that the client placed such an order. And thirdly, the access of unauthorised persons will be limited so that they will not be able to place any orders from a client's account. As it was mentioned before, simple and one-off passwords protect from only third threat, it is they limit the assess of unauthorised persons. Nevertheless, the passwords do not provide a bank and a client with the confirmation of the realised transaction. The passwords are not at all bound with the transaction's data. In case of the electronic signature, an abbreviation of information is created. That abbreviation includes the most important data concerning the amount of the transaction and the numbers of accounts – the charged account and the target one.

The enquiry titled "The Assessment of Safety Level of Electronic Financial Transactions" is one of important elements of my doctors thesis. The aim of that enquiry was defining the level of respondent's knowledge of the safety of communication in electronic transactions done through the Internet. The questionnaire consisted of four parts. Two of them concerned statistic data like respondent's characteristics and the summary of process of filling in the questionnaire. The remaining two parts contained questions about electronic banking and the electronic signature, one of those parts was directed only to the respondents, who use Internet banking. The research showed that the respondents were

using the electronic signature or coding the data transmission when they were doing trade or financial transactions, however they were not aware of that. The reason was connected with technical aspects – a part of process of authorising the user in the electronic communication was done by computer program in “the background”. The user was informed only about an error if it occurred. Hence, the conclusions are worrisome, because they show that the unaware users are potential, easy target of hackers’ attacks.

78% of respondents have heard about the electronic signature, while the half of respondents were acknowledged with the subject matter of the electronic banking and therefore filled in the third part of the questionnaire. 48% out of those last mentioned respondents reckoned that the usage of the electronic signature will increase the safety of communication in the electronic transactions. Only 8% stated that it will not. The population examined in the questionnaire showed interest in getting the electronic signature in the future. The answers received in the enquiry are presented in the table 1.

Table 1. The wish of respondents to obtain the electronic signature

	The percentage of respondents
Absolutely yes	12,6%
Rather yes	32,6%
It is hard to say	42,1%
Rather not	6,3%
Absolutely not	3,2%
I have already had an electronic signature	3,2%
Total	100,0%

Source: own work on the basis of enquiry research.

The results gathered on the basis of enquiry showed that the age of respondents was the characteristic which determined the usage of new electronic techniques. Moreover, apart from the age, the level of education occurred to be another factor which influences the level of knowledge of security methods connected with electronic transactions.

Due to technical structure of the electronic signature and the safety guarantee which it offers, the electronic signature is an ideal tool to secure the communication in Internet banking. The client who owns secure electronic signature can be sure that his orders are appropriately

protected at the moment on transmission to the bank. Similarly, the bank has a guarantee that the transaction was done by its client.

3.3. The perspectives of usage

The secure electronic signature can be bought through one of three certification centres. The registry of qualified entities is run by the National Bank of Poland. There are in the registry: Krajowa Izba Rozliczeniowa SA, Polska Wytwórnia Papierów Wartościowych SA, Unizeto Technologies SA. Those entities offer secure electronic signature through their sales offices and brokers.

In the opinion of specialists, the secure electronic signature guarantees the highest level of security in electronic communication, although one can observe the stagnancy in its usage. Media state that the banks will decide on the future of the electronic signature – either they will disseminate it, or they will diminish its usage. Bank Nordea is one of the pioneers in implementing modern solutions of IT safety. It was one of the first banks which introduced in 2006 the possibility of using the secure electronic signature in communication with the bank³². Moreover, Bank Nordea gave its clients the possibility to buy the electronic signature in selected bank branches.

For those who prefer full mobility and for whom carrying the electronic signature on a microprocessor card could be a problem, the company MobiTrust wants to launch a secure electronic signature set through mobile phone. The signature will be stored not on the microprocessor card, but on phone's SIM card.

Apart from guaranteeing the communication in electronic banking, the electronic signature has also huge perspectives of development in the economic world. It can be used in:

- settlements with the Social Insurance Company,
- placing documents and applications to public offices and public administration organs,
- issuing electronic invoices,
- taking part in electronic auctions and tenders,
- communication with contracting party.

³² <http://www.nordea.pl/klienci-indywidualni/bankowosc-elektroniczna-nordea/podpis-elektroniczny.html> (20.07.2009).

The electronic invoices deserve more attention, as they gained significant popularity in the world, especially in big enterprises. The reason was their electronic character, which resulted in reducing the quantity of sales documentation. Nevertheless, according to the ordinance of the Ministry of Finance³³, in order to be able to send such an invoice, one has to guarantee the authenticity of its origin and integrality using the secure electronic signature or transmission of the electronic data (EDI). Receiving the electronic invoices does not oblige the receiver to have the electronic signature. The receiver only has to accept getting such invoices. The electronic invoices have to be kept in an archive just like paper invoices and they are given accessible in electronic way to the tax organs. Apart from the advantages of electronic documents, electronic invoices have additional positive aspect concerning setting the date of payment – the date of issuance and the date of delivery are the same. In case when the payment term results from the date of delivery, such kind of invoice accelerates significantly the term of payment from the contracting party. That easiness of setting the date of issuance and delivery of an invoice is also helpful in settlements of VAT.

Recent months indicated on unfavourable changes for the electronic signature in Polish legislation. The Ministry of Finance gave legal persons the possibility to settle the income tax for 2008 in yearly statement PIT-37 in electronic way through Internet without the necessity to confirm the data with a secure electronic signature. The authors of the change in law convinced that due requirement to sign the statement with the secure electronic signature, that kind of statement gained little popularity³⁴. That direction of changes in legislation is a real threat to such an instrument as the electronic signature.

References

Cellary W., *Polska w drodze do globalnego społeczeństwa*, Program Narodów Zjednoczonych ds. Rozwoju, Warszawa 2002.

³³ Rozporządzenie Ministra Finansów z 14 lipca 2005 r. w sprawie sposobu i warunków wystawiania oraz przesyłania faktur w formie elektronicznej, a także zasad przechowywania oraz trybu udostępniania organowi podatkowemu lub organowi kontroli skarbowej faktur przesłanych drogą elektroniczną (Dz.U. z 2005 r. Nr 133, poz. 1119).

³⁴ <http://www.mf.gov.pl/dokument.php?const=3&dzial=205&id=165289&typ=news> (05.05.2009).

Dyrektywa 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz.Urz. WE L 13 z 19.01.2000).

Dziuba D., *Systemy informatyczne w obsłudze banków detalicznych*, Katedra Informatyki Gospodarczej i Analiz Ekonomicznych Wydziału Nauk Ekonomicznych Uniwersytetu Warszawskiego, Warszawa 2002.

Gospodarowicz A., *Bankowość elektroniczna*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2005.

Górka J., *Specyfika ryzyka bankowości elektronicznej, Materiały i studia*, Zeszyt nr 205, Narodowy Bank Polski, Warszawa 2006.

Grzechnik J., *Bankowość internetowa*, Internetowe Centrum Promocji, Gdańsk 2000.

Janc A., Kotliński G., *Nowe technologie we współczesnym banku*, Akademia Ekonomiczna w Poznaniu, Poznań 2004.

Janc A., Kotliński G., *Wykorzystanie bankowości elektronicznej w rozwoju usług*, „Bank” 1999, nr 9.

Jurkowski A., *Bankowość elektroniczna, Materiały i studia*, Zeszyt nr 125, Narodowy Bank Polski, Warszawa 2001.

Koterwas M., *Bazylejski Komitet ds. Nadzoru Bankowego i jego wpływ na kształt nadzoru bankowego na świecie*, „Bank i Kredyt” 2003, nr 10.

Koźliński T., *Bankowość internetowa*, CeDeWu, Warszawa 2004.

Maćkowiak K., *Bankowość elektroniczna – korzyści i zagrożenia*, „BOSTON IT Security Review” 2007, nr 4.

Marcinkowska M., *WAPorujące usługi bankowe*, „Bank” 2001, nr 1.

Newell F., *Lojalność.com*, IFC Press, Kraków 2002.

Pacholski L., Trzcieliński S., *Koncepcje zarządzania przedsiębiorstwem*, Instytut Inżynierii Zarządzania Politechnika Poznańska, Poznań 2003.

Przetocki J., *Podpis elektroniczny. Komentarz do ustawy z 18 września 2001 roku*, Lexis Nexis, Warszawa 2002.

Przybylska-Kapuścińska W., Ziarko-Siwiek U., *Nowe usługi finansowe w Polsce*, Akademia Ekonomiczna w Poznaniu, Poznań 2002.

Raport I Kongresu Informatyki Polskiej, Poznań 1994, http://www.kongres.org.pl/online/1-szy_Kongres/index.html.

Rekomendacja D dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki, Generalny Inspektor Nadzoru Bankowego, Warszawa 2002.

Risk management for electronic banking and electronic money activities, Basle Committee on Banking Supervision, Basle, Marzec 1998.

Rozporządzenie Ministra Finansów z 14 lipca 2005 r. w sprawie sposobu i warunków wystawiania oraz przesyłania faktur w formie elektronicznej, a także zasad przechowywania oraz trybu udostępniania organowi podatkowemu lub organowi kontroli skarbowej faktur przesłanych drogą elektroniczną (DzU z 2005 r. Nr 133, poz. 1119).

Świecka B., *Bankowość elektroniczna*, CeDeWu, Warszawa 2004.

Tomala P., *Systemy home bankingowe*, „Bank” 2002, nr 7-8.

Ustawa z dnia 12 września 2002 roku o elektronicznych instrumentach płatniczych (DzU z 2002 r., nr 169 poz. 1385).

Ustawa o podpisie elektronicznym z dnia 18 września 2001r., (DzU Nr 130, poz. 1450).

www.ingbank.pl/u235/navi/56117

www.lukasbank.pl/oferta_ekonto_bezpiecz_token.asp

www.mbank.pl/przewodnik/bezpieczenstwo/porwnanie_hasel_kodow.html

media.pekao.com.pl/pr/28659/historia-banku-pekao-sa-w-pigulce

www.nordea.pl/klienci-indywidualni/bankowosc-elektroniczna-nordea/podpis-elektroniczny.html